

OECD Global Forum on Policy Frameworks for the Knowledge-Based Economy: ICTs, Innovation, and Human Resources

September 16-17, 2002

Brasilia, Brazil

Statement by Joseph Richardson

Thank you, Mr. Chairman: I am pleased to be here today to take part in this timely and important dialogue on the policy frameworks for the knowledge-based economy. Today I would like to address two inter-related sets of policy issues that impact the diffusion of the knowledge based economy. The first is the policy framework for infrastructure development. The second is a framework to build trust in the use of information systems, the policy framework for cyber security.

Our discussion of the knowledge-based economy is part of a larger global dialogue -- how to encourage the use of information-based technologies to meet basic development goals and to thereby promote economic and social opportunities for all the world's citizens.

Remarkable strides have been made over the last two decades.

Access to information technologies has been dramatically increasing around the world. The number of mobile subscribers expanded from 491 million in 1999 to approximately 950 million by the end of 2001 - an extraordinary increase in only two short years. Internet users have increased from 200 million in September 1999 to 580 million in May 2002. And, Internet users within developing countries now represent some 20% of all Internet users.

Much of this growth is because people are obtaining new and better telecommunications services at much lower prices.

Progress, however, should not be an excuse for complacency. The gap between developed and developing countries, and among different socio and economic groups in individual countries persists. We are convinced that political and economic reforms are crucial if all countries are to seize the benefits of the ICT revolution.

A global consensus is emerging around four fundamental principles that provide the basis for ICT development:

1. liberalization and competition
2. commitment to the rule of law
3. private sector-led innovation
4. human capacity building

At the ITU's World Telecommunication Development Conference last March, over 150 countries affirmed these general principles when they approved the Istanbul Action Plan.

The commitment to liberalization and competition in the ICT sector opens the door to productivity gains and sustainable wealth creation through increased private investment.

Only the private sector has the flexibility and resources to offer innovative solutions to the unique problems facing ICT deployment. As a recent OECD report indicates, countries that build an environment conducive to private sector investment and adaptable to technological innovation experience the greatest benefits of the networked economy.

But investment funds will only flow into those economies that establish administrative and commercial institutions based on predictable and transparent rules, especially good governance. Companies, both domestic and foreign, require assurances that regulations are transparent and fair, and that contracts will be enforced - in a word, that there is a sound, legal basis for commercial investment.

Lastly, investment is broader than simply capital flows. It includes investment in people. ICT training and educational initiatives are the cornerstone of expanded access and usage of information-based technologies.

Once the policy framework for infrastructure development is in place, a policy framework to build trust in the use of information systems must also be put into place. Key among these frameworks are policies to support trust on the Internet, one of which is a policy infrastructure to provide security.

You know there are vulnerabilities and you know there are economic losses due to misuse of the Internet. But a few numbers highlight the problem. The CERT Coordination Center's statistics show that the number of incidents reported has increased from 10,000 in all of 1999 to 43,000 in the first half of 2002.

The threats are becoming more malicious. Viruses and worms have replaced hoaxes and jokes as the largest proportion of reported threats.

Damages are also rising. In 2000 the "I love you" virus is estimated to have caused US\$ 198 of damage per computer infected. In 2001, Nimda caused damage of US\$ 1,300 per infected computer.

Issues of trust are also very personal. The US Federal Trade Commission (FTC) reports that identity theft complaints (both online and off) are coming in at the rate of more than 13,000 per month, the single largest complaint category.

Addressing these issues will require every country to develop and implement a cyber security strategy. While every country's strategy will be unique, there must also be certain common characteristics based on the fact that the information systems and networks are interconnected globally across national borders.

The global experience with Y2K showed how important a point of contact is for international cooperation. Establishing national points of contact for cyber security would build on that experience.

Every national strategy for cyber security must be based on the enactment a comprehensive set of law and policy that includes substantive laws to criminalize misuse of the internet; procedural laws to lay out process involved; and laws and policies that allow cross-border information exchange related to enforcement. These laws and policies should meet or exceed the minimums outlined in the Council of Europe Cyber Crime Convention, the first multilateral instrument drafted to address threats to computer networks.

The increasing speed with which attacks spread around the world and the fact that criminal activity often crosses borders require new attention to cross border information sharing and cooperative initiatives. Legal enforcement and incident analysis and response each require a national point of contact that is trained and equipped, operates on a 7/24 basis, and has the ability to cooperate internationally. Because the private sector owns most of the critical infrastructures in any country, an effective public/private partnership for computer emergency response is essential.

Development and use of security standards and technical guidelines to enhance security deserve attention in a national strategy.

Raising Public Awareness as to the security threats and the roles and responsibilities for cyber security of all those involved with information systems and networks is a key area. The OECD "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" announced on August 7 provide an excellent basis for addressing public awareness. These nine common sense principles call for a new way of thinking about security, a new way of behaving towards communications systems. They are addressed to all participants involved with information systems and networks, from government and the largest corporations and institutions to individuals who connect with the Internet through a home PC.

A cyber strategy should also address Education and Training because there is great need and a global shortage of adequately trained personnel.

Finally, there is the issue of new technologies, exemplified by the current near absence of security for wireless devices connected to the Internet. We must

encourage developers and users of new technologies that connect to the information infrastructure to consider security as a fundamental requirement not an afterthought in the deployment of the technology.

In conclusion, the knowledge-based economy is dependent upon the buildout of the telecommunications infrastructure. A market oriented, private-sector led, liberal, competitive policy framework based in the rule of law, that includes the need for investments in human capital, has been shown to be an effective framework for infrastructure buildout. Full utilization of this network is dependent on the development of trust by users in that network. Trust in turn, requires security: a strategy that ensures a comprehensive set of laws to address misuse of the system, provisions for cross-border information exchange, utilization of appropriate standards, public outreach, education and training, and security for new technologies that will be attached to the network.